НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК 519.21

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“15” травня 2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 «Прикладна математика»

на тему: “ID-based” криптографічні протоколи із забезпеченням властивості анонімності ключа

Виконав (-ла): студент (-ка) 2 курсу, групи _____ФІ-63М_____
(шифр групи)

Рибак Богдан Сергійович

Керівник д.т.н. Кудін А.М.

-

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.т.н. Проскуровський Р.В.

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018року

РЕФЕРАТ

Роботу виконано на 52 аркушах, вона містить перелік посилань на використані джерела з 12 найменувань.

Метою даної дипломної роботи є побудова протоколу ID-based групового шифрування з лазівкою.

Об'єктом дослідження є надсилання повідомлень у групі користувачів

Предметом дослідження є протоколи анонімності отримувача засновані на ID-based шифруванні

Визначивши ключові аспекти можливого застосування, наведено мотивацію доцільності побудови протоколу ID-based групового шифрування з лазівкою. Запропоновано відповідний протокол. На основі наведеного визначення протоколу проведено аналіз його властивостей, зокрема коректності та безпеки. Було визначено модель безпеки та відповідність складових частин протоколу та протоколу в цілому цій моделі.

Результати роботи можуть бути використані для практичної реалізації запропонованої криптосистеми.

АНОНІМНІСТЬ КЛЮЧА, ГРУПОВЕ ШИФРУВАННЯ, ID-BASED

ABSTRACT

The thesis is presented in 52 pages. It contains bibliography of 12 references.

The **goal** of the thesis is the construction of the ID-based group encryption protocol with trapdoor.

The object is sending messages in the group of users

The subject are the ID-based protocols ensuring the property of receiver anonymity.

In the thesis, protocols which ensure the property of receiver anonymity are analyzed. After providing the motivation for possible use cases, the description of the ID-based group encryption protocol with trapdoor was provided. The analysis of correctness and other properties of the proposed protocol was conducted. The security model was established and the reasoning behind the protocol security in this model was provided.

Results of the work can be used for practical implementation of the proposed crypto system.

KEY ANONYMITY, GROUP ENCRYPTION, ID-BASED

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

$a \in_R \mathcal{A}$ — елемент a обрано з множини $\mathcal{A}$ рівноімовірно

$a, b \in_R \mathcal{A}$ — елементи a, b обрано з множини $\mathcal{A}$ незалежно і рівноімовірно

CDH — обчислювальне припущення Діффі-Геллмана (Computational Diffie–Hellman assumption) [1]

CcoDH — обчислювальне ко-припущення Діффі-Геллмана (Computational Diffie–Hellman co-assumption) [1]

ВСТУП

Актуальність роботи. Класична асиметрична криптографія, початком якої вважаються роботи Діффі та Геллмана [2], Меркле [3] та Рівеста, Шаміра та Адлемана [4], використовується в основному для вирішення двох задач:

– Забезпечення цифрового підпису повідомлення

– Забезпечення секретності вмісту повідомлення

За десятиліття що пройшли з моменту публікації Шаміра з'явилось і широко використовується багато перевірених, в тому числі й теоретично, криптографічних протоколів, що призначені вирішити вищенаведені задачі. Втім, існують класи проблем, що не покриваються ними. Це, зокрема, забезпечення анонімності *отримувача* повідомлення та забезпечення комплексного динамічного контролю доступу користувача до якогось ресурсу без необхідності користувачу розкривати власну ідентичність на кожному кроці.

ID-based шифрування вирішує у деяких контекстах проблему тотальної залежності від інфраструктури публічних ключів. Доцільним є поєднання ID-based шифрування із груповим.

У деяких випадках (зокрема, юридичних) корисною є можливість мати у шифротексті лазівку, яку можна розкрити для забезпечення можливості будь-кому чітко визначити, чи є шифротексти надісланими конкретній особі. При цьому не має компрометуватися приватність інших отримувачів та загальна стійкість схеми.

Метою роботи є побудова протоколу ID-based групового шифрування з лазівкою.

У ході дослідження ставляться наступні **завдання**:

– Дослідження існуючих протоколів, що забезпечують відправлення повідомлень із властивістю анонімності отримувача (анонімності ключа).

– Побудова власного протоколу надсилання повідомлень із забезпеченням властивості анонімності ключа, що має базуватись на ID-based шифруванні та мати лазівку для розкриття анонімності

– Доведення коректності і властивостей запропонованого протоколу.

Методи дослідження: методи математичного моделювання, теоретико-числових алгоритмів, теорії чисел.

Об'єкт дослідження: надсилання повідомлень у групі користувачів

Предмет дослідження: протоколи анонімності отримувача засновані на ID-based шифруванні

Наукова новизна одержаних результатів полягає у розробці протоколу ID-based групового шифрування з лазівкою

Практичне значення одержаних результатів полягає у можливості використання запропонованого протоколу у програмних продуктах, що мають забезпечувати відповідні протоколу властивості.

1 ОГЛЯД ПРОТОКОЛІВ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ ОТРИМУВАЧА

1.1 Мотивація задачі групового шифрування

Як вже було зазначено, класична асиметрична криптографія займається питаннями цифрового підпису та шифрування повідомлень. Але, попри дослідженість та широке використання, прості протоколи на кшталт цифрового підпису Діфі-Хелмана на еліптичних кривих або шифрування RSA не покривають і не можуть покрити усі можливі потреби людства у забезпеченні властивостей інформації за умови несиметричного до неї доступу.

Однією з таких потреб є забезпечення анонімності *отримувача* деякого повідомлення (тобто, забезпечення анонімності *ключа* шифрування). За умови можливості доведення факту, що цей отримувач належить певній групі осіб, така задача має декілька потенційних застосувань. Наведемо деякі приклади [5].

1. Застосування, пов'язані з анонімними довірчими третіми особами Багато протоколів, такі як протоколи чесного шифрування, чесного обміну, групових підписів тощо, покладаються на наявність деякої третьої особи — *доручителя*, до якої звертаються лише у випадку, коли нормальний хід протоколу порушується (наприклад, у протоколі чесного обміну одна із сторін не передала свою обіцяну власність іншій).

Для таких протоколів можливою (інколи навіть бажаною) є ситуація, у

який таких можливих доручителів більше за одного. У цьому випадку сам факт вибору стороною протоколу конкретного доручителя може призвести до витоку небажаної інформації про особу даної сторони. Наприклад, уявимо ситуацію, коли система identity escrow є міжнародно визнаною і у кожної країни є свій національний учасник такої системи. Тоді учасник може хотіти (або бути зобов'язаним законом) обрати доручителя саме з його власної країни. Факт такого вибору розкриває інформацію про місцезнаходження учасника, що може бути небажаним.

2. Захищена передача даних між пристроями. У сучасних умовах великої кількості різноманітних персональних та комерційних обчислювальних пристроїв передача даних між ними є неординарним питанням. Уявимо ситуацію, у якій користувач хоче використати деякий хмарний ресурс для переміщення даних з одного пристрою на інший. При цьому на який саме пристрій переміщуються дані не розкривається. В той самий час вищезгаданий хмарний ресурс може хотіти підтвердження, що дані переміщуються дозволеним учасником на один з дозволених пристроїв, щоб уникнути зберігання зайвої інформації. Забезпечення анонімності адресата повідомлення разом із підтвердженням його належності до деякої групи можна вважати рішенням даної задачі із забезпеченням необхідного рівня приватності.

3. Відправлення повідомлень державним правоохоронним агенціям. За наявності інформації про конкретного адресата (агенції чи конкретної людини) деякого компрометуючого повідомлення, зловмисник має змогу впливу безпосереднього на адресата, що підвищує ймовірність успіху зловмисника і зменшує ефективність охорони права.

Отже, як можна побачити, задача групового шифрування з підтвердженням має цінність для практичного забезпечення деяких властивостей інформації у певних контекстах.

1.2 Деякі теоретичні відомості

1.2.1 Обчислювальні припущення

Наведемо визначення деяких обчислювальних припущень, що будуть використовуватися надалі.

Визначення 1.1. *Нехай X_n - ансамбль n незалежних випадкових величин, породжений розподілом P_x, Y_n - ансамбль n незалежних випадкових величин, породжений розподілом P_y.*

Розподіли P_x та P_y називаються обчислювально нерозрізнюваними у сенсі параметра α, якщо для будь-якого поліноміального відносно α ймовірнісного алгоритму A:

$$\forall n_0 > 0 \quad \exists c \in \mathbb{R} : \quad \forall n > n_0 \quad |P[A(X_n) = 1] - P[A(Y_n = 1)]| < \frac{1}{\alpha^c},$$

Припущення 1.2. *Розглянемо циклічну мультиплікативну групу $\mathbb{G}$ порядка q із генератором g. Кажуть, що у групі $\mathbb{G}$ виконується* вибіркове припущення Діффі-Хеллмана *(Decisional Diffie-Hellman Assumption), якщо*

розподіли наступні двох груп величин є обчислювально нерозрізнюваними (у сенсі параметра $n = \log q$*):*

- $\left(g^a, g^b, g^{ab}\right)$*, якщо* $a, b \in_R \mathbb{Z}_q$*.*
- $\left(g^a, g^b, g^c\right)$*, якщо* $a, b, c \in_R \mathbb{Z}_q$*.*

1.2.2 Білінійні пари

Оскільки велика частина протоколів побудована на примітиві абстрактної алгебри під назвою *білінійна пара* (Bilinear pairing), має сенс розглянути більш детально цей примітив та його властивості.

Визначення 1.3. $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$ *— ефективне білінійне відображення, якщо виконуються наступні умови:*

а) ***Невиродженість:*** $e(g_1, g_2) \neq 1$

б) ***Білінійність:*** $\forall h_1 \in \mathbb{G}_1, h_2 \in \mathbb{G}_2, u, v \in \mathbb{Z} : e(h_1^u, h_2^v) = e(h_1, h_2)^{uv}$

З білінійними відображеннями тісно пов'язане наступне обчислювальне припущення:

Припущення 1.4. *Розглянемо пару циклічних мультиплікативних груп* $\Delta = \langle \mathbb{G}_1, \mathbb{G}_2 \rangle$ *Кажуть, що для пари* Δ *виконується* зовнішнє припущення Діффі-Хеллмана *(eXternal Diffie-Hellman Assumption), якщо виконуються наступні умови:*

- *Проблема дискретного логарифму є складною у* $\mathbb{G}_1, \mathbb{G}_2$*.*
- *CDH виконується у* $\mathbb{G}_1, \mathbb{G}_2$*.*
- *CcoDH виконується у* $\mathbb{G}_1, \mathbb{G}_2$*.*

– *Існує ефективне білінійне відображення* $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.

– *Вибіркове припущення Діффі-Хеллмана виконується у* $\mathbb{G}_1$.

Нехай існує кортеж $\Gamma = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3, g_1, g_2, e)$, де $\mathbb{G}_1 = \langle g_1 \rangle$, $\mathbb{G}_2 = \langle g_2 \rangle$, $ord(\mathbb{G}_1) = ord(\mathbb{G}_2) = p$, причому p — просте, e — ефективне білінійне відображення.

існує три типи таких кортежів:

а) $\mathbb{G}_2 = \mathbb{G}_1$. Для таких випадків позначення кортежа спрощується до $\Gamma = (p, \mathbb{G}_1, \mathbb{G}_3, g, e)$.

б) $\mathbb{G}_2 \neq \mathbb{G}_1$, причому існує *ефективне спотворююче відображення* $\psi : \mathbb{G}_2 \to \mathbb{G}_1$, але не існує *ефективного* спотворюючого відображення $\phi : \mathbb{G}_1 \to \mathbb{G}_2$; тут спотворююче відображення задовольняє умові $\forall u \in \mathbb{Z}_p : \psi(g_2^u) = \psi(g_2)^u \in \mathbb{G}_1$.

в) $\mathbb{G}_2 \neq \mathbb{G}_1$, але не існує ні *ефективного* спотворюючого відображення $\phi : \mathbb{G}_1 \to \mathbb{G}_2$, ні *ефективного* спотворюючого відображення $\psi : \mathbb{G}_2 \to \mathbb{G}_1$.

1.2.3 Додаткові обчислювальні припущення

Із білінійними парами пов'язані три додаткових обчислювальних припущення, наведених далі

Припущення 1.5. *Розглянемо циклічну мультиплікативну групу* $\mathbb{G}$ *порядка* q *із генератором* g. *Кажуть, що для груп* $\mathbb{G}, \mathbb{G}_T$ *та ефективного білінійного відображення* e *виконується* Вибіркове білінійне експоненційне q-припущення Діфі-Геллмана *(q Decisional Bilinear Diffie-Hellman Exponent Assumption, q-BDHE), якщо, маючи на вході вектор з* $2q + 1$ *елемента:*

$$\left(g',g,g^{\alpha},g^{\alpha^2},\ldots,g^{\alpha^q},g^{\alpha^{q+2}},\ldots,g^{\alpha^{2q}}\right) \in \mathbb{G}^{2q+1}$$

,

неможливо обчислити за поліноміальний час $e\left(g,g'\right)^{\alpha^{q+1}} \in GT$.

Припущення 1.6. *Розглянемо циклічну мультиплікативну групу* $\mathbb{G}$ *порядка* q *із генератором* g. *Кажуть, що для груп* $\mathbb{G},\mathbb{G}_T$ *та ефективного білінійного відображення* e *виконується* Доповнене вибіркове білінійне експоненційне q-припущення Діфі-Геллмана *(q Augmented Decisional Bilinear Diffie-Hellman Exponent Assumption, q-ABDHE), якщо, маючи на вході вектор з* $2q+2$ *елементів:*

$$\left(g',g'^{\alpha^{q+2}},g,g^{\alpha},g^{\alpha^2},\ldots,g^{\alpha^q},g^{\alpha^{q+2}},\ldots,g^{\alpha^{2q}}\right) \in \mathbb{G}^{2q+2}$$

,

неможливо обчислити за поліноміальний час $e\left(g,g'\right)^{\alpha^{q+1}} \in GT$.

Припущення 1.7. *Розглянемо циклічну мультиплікативну групу* $\mathbb{G}$ *порядка* q *із генератором* g. *Кажуть, що для груп* $\mathbb{G},\mathbb{G}_T$ *та ефективного білінійного відображення* e *виконується* Обрізане доповнене вибіркове білінійне експоненційне q-припущення Діфі-Геллмана *(q Truncated Augmented Decisional Bilinear Diffie-Hellman Exponent Assumption, truncated q-ABDHE), якщо, маючи на вході вектор з* q *елементів:*

$$\left(g',g'^{\alpha^{q+2}},g,g^{\alpha},g^{\alpha^2},\ldots,g^{\alpha^q}\right) \in \mathbb{G}^{q}$$

,

неможливо обчислити за поліноміальний час $e\left(g,g'\right)^{\alpha^{q+1}} \in GT$.

Визначення обрізаного доповненого вибіркового білінійного експоненційного q-припущення Діфі-Геллмана є тривіальним окремим випадком визначення доповненого вибіркового білінійного експоненційного q-припущення Діфі-Геллмана.

1.3 Огляд існуючих протоколів групового шифрування

1.3.1 Протокол Кояса

У 2007 році Коясом et al. було представлено роботу під назвою “Group Encryption” [5], у якій було вперше запропоновано поняття анонімності отримувача повідомлення у асиметричних криптосистемах, надано визначення та запропоновано модель протоколів групового шифрування, та запропоновано приклад такого протоколу із обґрунтуванням його безпеки. Розглянемо їхні напрацювання більш детально.

Учасниками схеми групового шифрування у визначенні Кояса et al. є чотири сторони:

– Менеджер групи, який адмініструє групу

– Зареєстровані члени групи, які анонімно отримують повідомлення

– Доручитель, який може відкривати ідентичність отримувача

– Верифікатор, який може перевірити правильність протоколу без знання секретів

Формально, **схема групового шифрування Кояса** для відношення(групи

користувачів) R — це набір таких процедур:

а) **SETUP**

б) **JOIN**

в) $\langle \mathcal{G}_r, R, Sample_R \rangle$

г) **ENC**

д) **DEC**

е) **OPEN**

є) $\langle \mathcal{P}, \mathcal{V}, recon \rangle$

Опишемо функціональність цих процедур і загальний вигляд схеми.

– SETUP — це набір трьох процедур ініціалізації протоколу: для публічних параметрів системи, для Менеджера групи (GM) та для доручителя(OA) ($SETUP_{init}$, $SETUP_{GM}$ та $SETUP_{OA}$ відповідно). Використовуючи відповідні процедури, Менеджер та доручитель генерують власні ключові пари $\langle pk_{GM}, sk_{GM} \rangle$ та $\langle pk_{OA}, sk_{OA} \rangle$.

– JOIN = $\langle J_{user}, J_{GM} \rangle$ — набір протоколів для спілкування потенційного учасника групи та Менеджера. Після виконання JOIN новий учасник групи має свою ключову пару $\langle pk, sk \rangle$. Публічний ключ p_k нового учасника разом із сертифікатом $cert$ публікується Менеджером у публічній базі даних $database$ учасників групи.

– Процедура $\mathcal{G}_r(1^\nu)$ генерує з параметрів відношення R пару $\langle pk_R, sk_R \rangle$.

– Для проведення транзакції Відправник отримує пару (x, w) за допомогою алгоритму $Sample_R(pk_R, sk_R)$. При цьому поліноміальна процедура перевірки $R(x, w)$ має повертати “так” тоді і тільки тоді, коли (x, w) належить до відношення із публічним параметром pk_R.

– Маючи пару (x, w) Відправник бажає зашифрувати w для обраного

Отримувача. Для цього Відправник отримує публічний ключ Отримувача $\langle p_k, cert\rangle$ з публічної бази даних та за допомогою публічних ключів pk_{GM} та pk_{OA} шифрує w як $ENC(pk_{GM}, pk_{OA}, pk, w, L)$ для отримання шифротексту ψ з деякою позначкою L. (де L - публічний рядок, прив'язаний до шифротексту).

– Для проведення перевірки, Відправник та Верифікатор приймають участь у алгоритмі доведення без розголошення $\langle \mathcal{P}, \mathcal{V}, recon\rangle$, у якому буде доведено наступне щодо шифротексту ψ та позначки L: існує член групи, чий ключ є зареєстрованим у базі даних, що здатен розшифрувати ψ в контексті L та отримати значення w', для якого справедливо наступне: якщо $w \leftarrow recon(w')$, то $(x, w) \in R$. Тут функція $recon$ реконструює свідка, базуючись на розшифруванні ψ і може бути тотожним відображенням.

Загальний вигляд схеми наведемо без змін відповідно до [5].

Визначення 1.8. *(коректність) Схема групового шифрування є коректною, якщо наступна гра майже напевно повертає 1:*

а) $param \leftarrow SETUP_{init}(1^\nu)$;

$\langle pk_R, sk_R\rangle \leftarrow \mathcal{G}_r(1^\nu); (x, w) \leftarrow sample_R(pk_R, sk_R)$.

б) $\langle pk_{GM}, sk_{GM}\rangle \leftarrow SETUP_{GM}(param)$;

$\langle pk_{OA}, sk_{OA}\rangle \leftarrow SETUP_{OA}(param)$.

в) $\langle pk, sk, cert|pk, cert\rangle \leftarrow \langle J_{user}, JGM(sk_{GM})\rangle (pk_{GM})$. *Якщо* $pk \notin \mathcal{L}_{pk}^{param}$, *перериваємо виконання.*

г) $\psi \leftarrow ENC(pk_{GM}, pk_{OA}, pk, cert, w, L)$.

д) $out_1 \leftarrow w \stackrel{?}{=} recon(DEC(sk, \psi, L))$

е) $out_2 \leftarrow pk \stackrel{?}{=} OPEN(sk_{OA}, [\psi]_{oa}, L)$

є) $\langle done|out_3\rangle \leftarrow \langle \mathcal{P}(w, \psi, coins_\psi), \mathcal{V}\rangle$

$(param, pk_{GM}, pk_{OA}, pk_R, x, \psi, L)$.

ж) Якщо $out_1 = out_2 = out_3 = true$*, повертаємо 1.*

Для систем групового шифрування [5] визначає три аспекти безпеки:

- Секретність.
- Анонімність.
- Стійкість(міцність).

Ці аспекти формулюються в термінах ігр та оракулів без стану. Ці визначення в рамках даної роботи наводитись не будуть.

У роботі [5] також було запропоновано конкретну побудовану схему групового шифрування на основі відомих криптопримітивів та проведено оцінку її стійкості. Для практичної реалізації схеми у подібній моделі необхідно, щоб криптопримітиви підтримували обчислювально просте доведення без розголошення.

Кояс et al. пропонують використовувати криптосистему Пальє та отримують систему, стійку до адаптивних атак із обраним шифротекстом без використання у доведенні випадкових оракулів. Протокол доведення без розголошення у даній криптосистемі є інтерактивним.

1.3.2 Group decryption

У 2007 році Qin et al. [6] запропонували іншу назву схеми групового шифрування: групове розшифрування (Group decryption). Назва була змінена на групове розшифрування задля наголошення на анонімності отримувача. Робота наводить також конкретну криптосистему, яка згідно до авторів є

більш ефективною за систему Кояса et al.

Учасниками цієї процедури згідно до роботи є чотири сторони:

– Менеджер групи, який адмініструє групу

– Зареєстровані члени групи, які анонімно отримують повідомлення від авторів

– Автор(и) повідомлень, які можуть як бути так і не бути членами групи

– Перевіряючий, що може перевірити правильність протоколу без знання секретів

У їхньому визначенні, така схема (GE Scheme) складається з чотирьох процедур:

– **ParaGen** — поліноміальний у часі алгоритм, що на вході отримує параметр безпеки λ, а на виході продукує системні параметри π.

– **GKeyKen** — поліноміальний у часі алгоритм, що на вході отримує системні параметри π, а на виході продукує публічний та секретний ключі групи $(g_{pk}, g_{sk}$.

– **UKeyGen** — поліноміальний у часі алгоритм, що на вході отримує системні параметри π, а на виході продукує публічний та секретний ключі користувача $(u_{pk}, u_{sk}$. На однакових входах для різних запусків цей алгоритм продукує *різні* ключі.

– **Join** — поліноміальний у часі інтерактивний алгоритм, між користувачем $\mathcal{U}$, що хоче приєднатися до групи та менеджером групи $\mathcal{GM}$. Користувач має вхід u_{sk}, а менеджер групи - g_{sk}. Спільним для них входом є (π, u_{pk}, g_{pk}).

1.3.3 Групове шифрування із лазівкою

Групове шифрування із лазівкою (Traceable group encryption) [7] — схема, запропонована Лібером та ін. у 2014 році. Автори пропонують практичну систему групового шифрування з таємним входом, яка дозволяє менеджеру групи або авторизованій особі розкривати за потреби анонімність всіх шифротекстів, надісланих конкретній особі, без розкриття анонімності інших адресатів (що не підтримується традиційними схемами групового шифрування, які були описані).

Схема побудована на шифруванні Лібера-Янга [7], яке є варіантом шифрування Крамера-Шоу. У схемі групового шифрування із лазівкою для розподілу ключів використовується інфраструктура публічних ключів (Public Key Infrastructure). Для забезпечення розкриття ідентичності менеджером групи, частина ідентичності отримувача шифрується окремим ключем .

Розкриття анонімності конкретного користувача досягається за допомогою додавання лазівки, а саме:

– Кожен член групи, який бажає отримувати повідомлення, генерує два випадкові числа $a, b \in_R \mathbb{Z}_p$. Елементи g^a, g^b вважаються частиною публічного ключа користувача, а g^{ab} — приватного.

– При відправлені повідомлення вимагається наявність певної визначеної функції від g^a, g^b у шифротексті.

– Для розкриття анонімності конкретного отримувача менеджеру групи достатньо розкрити частину його приватного ключа g^{ab}.

1.3.4 ID-based групове шифрування

У 2016 році Луо та ін. було запропоновано схему ID-based групового шифрування (Identity-based group encryption [8]).

Дана робота пропонує систему групового шифрування, яка, на відміну від раніше описаних, не покладається на інфраструктуру публічних ключів. Натомість запропонована система використовує шифрування на основі ідентифікації (ID-based encryption).

Схема побудована модульно. У процесі шифрування за нею окремо шифрується шифротекст, використовуючи осліплений ідентифікатор користувача $s * ID$. Окремими блоком шифрується ідентичність користувача за допомогою криптосистеми з відкритим ключем Крамера-шоу.

Однаковість зашифрованого ідентифікатору користувача і ідентифікатору, з яким було зашифровано шифротекст, забезпечується за допомогою протоколу доведення без розголошення. Запропонований протокол є інтерактивним, втім, автори навели приклад трансформації його в неінтерактивний за допомогою геш-функції.

Безпеку системи авторами було доведено у стандартній моделі.

Висновки до розділу 1

У даному розділі було розглянуто математичні примітиви, що використовуються у протоколах забезпечення анонімності ключа шифрування та існуючі протоколи забезпечення анонімності ключа шифрування. Особливу увагу становить так зване групове шифрування, у якому отримувачі є членами деякої групи, причому так званий адміністратор даної групи відповідає за доведення коректності шифрування, а також за управління групою: додавання, виключення учасників тощо.

Було розглянуто роботи, що поєднують групове шифрування із ID-based шифруванням. Це дозволяє позбутись інфраструктури публічних ключів, що може бути доцільним у певних контекстах. Також було наведено опис протоколу групового шифрування з лазівкою, що дозволяє адміністратору групи розкрити анонімність шифротекстів для деякого учасника групи.

2 ГРУПОВЕ ID-BASED ШИФРУВАННЯ З ЛАЗІВКОЮ

2.1 Мотивація конструкції

У попередньому розділі вже була доведена доцільність звичайної задачі групового шифрування (анонімності отримувача). Цю схему можна змінити та розширити для набуття нею нових властивостей.

1. Доцільно роглянути використання ID-based шифрування замість інфраструктури публічних ключів. Класичною працею з ID-based шифрування є [9]. Основною перевагою такого методу асиметричного шифрування є можливість надсилати шифровані повідомлення, знаючи лише інформацію про ідентичність користувача (назва Identity-Based Encryption вказує саме на це).

У контексті групового шифрування ID-based шифрування було досліджене у [8]. Така схема може мати переваги над схемою з інфраструктурою публічних ключів у зручності та ефективності. Луо та ін. [8] довели безпеку схеми ID-based групового шифрування у стандартній моделі без використання випадкових оракулів. Це дозволяє базувати побудову схем ID-based групового шифрування на цих результатах без зменшення захищеності.

2. У деяких випадках (зокрема, юридичних) корисною є можливість мати у шифротексті лазівку, яку можна розкрити для забезпечення можливості будь-кому чітко визначити, чи є шифротексти надісланими конкретній особі.

Це може бути потрібно, наприклад, для більш ефективного використання ресурсів, адже у іншому випадку менеджеру групи доведеться власноруч перебирати всі надіслані повідомлення, що може бути обчислювально складно. При цьому не має компрометуватися приватність інших отримувачів та загальна стійкість схеми.

Далі буде запропоновано схему ID-based групового шифрування з лазівкою, наведено визначення безпеки та доведено її безпеку згідно із визначеннями, у стандартній моделі без використання випадкових оракулів.

2.2 Схема групового ID-based шифрування з лазівкою

2.2.1 Модель

Запропонована система виділяє п'ять окремих ролей:

а) Адміністратор групи (GM), який керує групою та розкриває ідентичність отримувачів у разі потреби.

б) Група користувачів, які отримують повідомлення без розкриття власної ідентичності

в) Відправник (може бути будь-хто), який власне надсилає зашифровані повідомлення.

г) Перевіряючий, який може довести, що шифротекст сформовано правильно і зашифрована особа отримувача співпадає з тою, чиїм ключем був зашифрований шифротекст.

д) Генератор приватних ключів (PKG), який може генерувати приватні ключі користувачів з публічних.

Ці ролі взаємодіють у рамках наступних процедур:

а) $ParaGen(\lambda)$ — Поліноміальний алгоритм, який викликається генератором приватних ключів. Він приймає на вхід параметр безпеки λ та повертає системні параметри $Params$ та головний приватний ключ MSK.

б) $GKGen(Params)$ — Поліноміальний алгоритм, який викликається адміністратором групи. Він приймає на вхід системні параметри $Params$ та повертає публічний та приватний ключі групи (PK_{GM}, SK_{GM}) відповідно.

в) $UKGen(Params, ID, MSK)$ — Поліноміальний алгоритм, який викликається генератором приватних ключів. Він приймає на вхід системні параметри $Params$, ідентифікатор користувача ID та секретний ключ MSK і повертає відповідний приватний ключ користувача SK_{ID}.

г) $Register(ID)$ — Поліноміальний алгоритм, який викликається адміністратором групи. Приймає на вхід ідентифікатор користувача ID і повертає інформацію, яку адміністратор зберігає для визначення, що такий ідентифікатор належить групі.

д) $Encryption(Params, M, ID, PK_{GM})$ — Поліноміальний алгоритм, який викликається відправником. Приймає на вхід ідентифікатор користувача ID, системні параметри $Params$, публічний ключ адміністратора PK_{GM} та відкритий текст M і повертає шифротекст C.

е) $Decryption(Params, C, SK_{ID})$ — Поліноміальний алгоритм, який

викликається отримувачем. Приймає на вхід приватний ключ користувача SK_{ID}, системні параметри $Params$, шифротекст C та повертає відкритий текст M.

є) $Trace(Params, C, SK_{GM})$ — Поліноміальний алгоритм, який викликається адміністратором групи. Приймає на вхід приватний ключ адміністратора SK_{GM}, системні параметри $Params$, шифротекст C та повертає "так"чи "ні"у залежності від правильності виконання шифрування ідентифікатору отримувача та його відповідності повідомленню.

Коректність схеми задається наступним визначенням:

Визначення 2.1. *Схема ID-based групового шифрування називається* коректною, *якщо наступна процедура повертає 0 з незначною ймовірністю:*

а) Будується набір $Params, MSK$ *за допомогою алгоритму ParaGen(*λ*).*

б) Запускається $GKGen(Params)$*, який повертає публічний та приватний ключі* (PK_{GM}, SK_{GM})*.*

в) Запускається $UKGen(ID, MSK)$*, який повертає приватний ключ* PK_{ID} *користувача з ідентифікатором* ID*.*

г) Запускається $Encryption(Params, M, ID, PK_{GM})$*, який повертає шифротекст* C

д) Якщо виконується:

$$((M \neq Decryption(SK_{ID}, C)) \vee$$
$$(\langle done|0\rangle \leftarrow \langle P(s,n,ID),\mathcal{V}\rangle$$
$$(C_{10},C_{11},g,g_1,g_2,g_3,k_1,k_2,\psi,l,t,w,d)) = 0)$$
$$\vee (ID \neq Trace\,(SK_{GM},C))$$

то повертається 0*, інакше повертається* 1.

2.2.2 Загальний опис

Запропонована схема групового шифрування з лазівкою є модульною. Вона включає в себе:

а) Схему ID-based шифрування для шифрування тексту повідомлення. Додатково на цьому етапі осліплюється ідентифікатор отримувача для забезпечення анонімності. У якості схеми ID-based шифрування тут використовується конструкція I (Construction I) з публікації Джентрі та ін. [10].

Ця конструкція для доведення секретності покладається на доповнене вибіркове білінійне експоненційне q-припущення Діфі-Геллмана, визначене в розділі 2 цієї роботи.

б) Схему ID-based шифрування для шифрування ідентифікатору отримувача. Особливістю даної складової в рамках цієї роботи є те, о окрім секретності за визначених умов, ця схема має забезпечувати лазівку, тобто

розкриття ідентичності конкретного отримувача (і тільки його) за бажанням менеджера групи. Для досягнення такиїх властивостей використовується аналогічна до попереднього пункту схема на основі конструкції I. Відмінностями її від першої є:

– Фіксованість відкритого тексту, який визначається опосередковано з ідентичності користувача.

– Інші параметри шифрування з окремою генерацією для забезпечення ізольованості цих двох складових загальної схеми групового ID-based шифрування з лазівкою.

в) Протокол доведення без розголошення для забезпечення перевірки ідентичності ідентифікаторів користувача у шифротекстах отриманих завдяки використанню зазначених вище схем. Цей протокол побудовано за допомогою конструкції так званого Σ-протоколу [11]. Конкретний Σ-протокол побудовано для виконання функцій, специфічних конкретній поданій схемі.

Особливістю даної схеми є можливість менеджеру групи дати можливість будь-кому перевірки, чи належить шифротекст конкретному користувачу з ідентифікатором ID, без запитів до менеджера групи. Для цього менеджер групи публікує:

а) Приватний ключ, що відповідає ідентифікатору ID для схеми шифрування для шифрування ідентифікатору отримувача.

б) Значення $e(g^{\dagger},g^{\dagger})^{ID}$, де $g^{\dagger}$ - параметр схеми шифрування для шифрування ідентифікатору отримувача.

При цьому анонімність інших учасників групи не компрометується.

Наведемо детальний опис запропонованої схеми та доведення безпеки та

коректності.

2.2.3 Детальний опис

Опишемо схему групового ID-based шифрування у вигляді процедур, визначених раніше.

а) $ParaGen(\lambda)$ — У даній процедурі для схеми, що розглядається, відбувається ініціалізація схеми групового шифрування для шифрування відкритого тексту повідомлення. Опишемо цю генерацію.

Нехай $\mathbb{G}, \mathbb{G}_T$ — дві групи порядку $p \in \mathbb{Z}$. Ідентифікатором користувача буде деяке $ID \in \mathbb{Z}_p$. Має існувати $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ — ефективне білінійне відображення. Обираємо:

$$g,h \in_R \mathbb{G}$$

$$\alpha \in_R \mathbb{Z}_p$$

$$g_1 \leftarrow g^{\alpha} \in \mathbb{G}.$$

Системні параметри та приватний ключ визначаються як, відповідно:

$$Params := (g,g_1,h)$$

$$MSK := \alpha.$$

Приватний ключ переходить у власність генератора приватних ключів (PKG), який, у загальному випадку, не співпадає із адміністратором групи, публічні

параметри є загальновідомими.

б) $GKGen(Params)$ — Проводимо процедуру, аналогічну до процедури $ParaGen$, оскільки використовується аналогічний криптографічний блок.

Обираємо:

$$g^{\dagger}, h^{\dagger} \in_R \mathbb{G}$$
$$\alpha^{\dagger} \in_R \mathbb{Z}_p$$
$$g_1^{\dagger} \leftarrow g^{\dagger\alpha^{\dagger}} \in \mathbb{G}.$$

Параметри групи та приватний ключ визначаються як, відповідно:

$$PK_{GM} := \left(g^{\dagger}, g_1^{\dagger}, h^{\dagger}\right)$$
$$SK_{GM} := \alpha^{\dagger}.$$

Приватний ключ переходить у власність адміністратора групи, публічні параметри є загальновідомими.

в) $UKGen(Params, ID, MSK)$ — Нехай ідентифікатором користувача є $ID \in \mathbb{Z}_p$ (методи перетворення ідентифікатору на число є тривіальними і виходять за рамки даної роботи). Встановлюємо:

$$r \in_R \mathbb{Z}_p, h_{ID} = \left(hg^{-r}\right)^{1/(\alpha - ID)}$$
$$SK_{ID} := (r, h_{ID}).$$

Значення SK_{ID} і є приватним ключем користувача з ідентифікатором ID.

г) $Encryption(Params, M, ID, PK_{GM})$ — Нехай відкритий текст —

$M \in \mathbb{G}_T$, ідентифікатор отримувача — $ID \in \mathbb{Z}_p$. Обирається випадкове $s \in_R \mathbb{Z}_p$. Шифрування відбувається у два етапи:

1) Шифрування повідомлення. Обчислюється:

$$C_{10} = g_1^s g^{-s \cdot ID}$$

$$C_{11} = e(g,g)^s$$

$$C_{12} = M \cdot e(g,h)^{-s}.$$

Шифротекстом цього етапу є триелементний кортеж

$$C_1 = (C_{10},C_{11},C_{12})\,.$$

2) Шифрування особистості отримувача. Обчислюється:

$$C_{20} = g_1^{\dagger s} g^{\dagger -s \cdot ID}$$

$$C_{21} = e(g^\dagger,g^\dagger)^s$$

$$C_{22} = e(g^\dagger,g^\dagger)^{ID} \cdot e(g^\dagger, h^\dagger)^{-s}.$$

Шифротекстом цього етапу є триелементний кортеж

$$C_2 = (C_{20},C_{21},C_{22})\,.$$

3) Результуючим загальним шифротекстом є:

$$C = (C_1,C_2) = (C_{10},C_{11},C_{12}, C_{20},C_{21},C_{22})\,.$$

д) $Decryption(Params, C, SK_{ID})$ — Нехай вхідний шифротекст

$C = (C_1, C_2)$, де $C_1 = (C_{10}, C_{11}, C_{12})$ згідно з визначеннями у пункті Encryption. Тоді відкритий текст можна отримати, як:

$$M = C_{12} \cdot e\left(C_{10}, h_{ID}\right) C_{11}^{r}$$

Доведення правильності розшифрування наведено у розділі 3.

е) $Trace(Params, C, SK_{GM})$ — Ця продедура дозволяє менеджеру групи відслідкувати отримувача за наявності деякого коректно сформованого шифротексту, або визначити некоректність шифротексту на вході. Вона частково покладається на протокол доведення без розголошення, описаний у пункті 2.2.4. Зараз про цей протокол необхідно знати лише те, що він повертає 0 у разі неспівпадіння ідентифікаторів у шифротекстах, інакше — повертає 1.

Менеджер групи може відслідкувати отримувача наступним чином:

– якщо процедура доведення без розголошення повертає 0, то повертаємо відмову,

– інакше обчислюємо $e(g^{\dagger}, g^{\dagger})^{ID} = DEC(C_2)$. Це можливо виконати, оскільки менеджер групи володіє генератором приватних ключів для схеми шифрування ідентичності.

Для всіх ідентифікаторів $ID_i \in I$, (де I - множина ідентифікаторів усіх зареєстрованих у даній групі користувачів) обчислюється $e(g^{\dagger}, g^{\dagger})^{ID}$ і порівнюється зі входом.

У випадку неспівпадіння жодного перетвореного ідентифікатору повертається відмова, інакше - знайдений ідентифікатор отримувача.

2.2.4 Протокол доведення без розголошення

У запропонованій схемі шифротекст складається із двох частин: зашифрованого повідомлення і зашифрованого ідентифікатору отримувача. Необхідною є можливість перевірити, що:

а) Перший і другий шифротексти відповідають одному й тому ж ідентифікатору користувача.

б) Шифротекст є правильним у цілому.

Для такої перевірки використовується протокол доведення без розголошення. Наведемо його опис.

Протокол доведення без розголошення побудовано за допомогою конструкції на основі так званих Σ-протоколів [11]. Наведемо визначення Σ-протоколу, разом з деякими допоміжними.

Визначення 2.2. *Бінарне відношення $R(x, w)$ — NP-відношення, якщо:*

а) Довжина w не перевищує $p(|x|)$, де p — деякий поліном, $|x|$ — довжина x.

б) Існує поліноміальний алгоритм перевірки належності довільної пари (x, w) відношенню R.

Визначення 2.3. *Протокол $\mathcal{P}$ має σ-структуру, якщо:*

а) Протокол $\mathcal{P}$ відбувається між двома учасниками P і V, які відповідають тому, хто доводить і тому, хто перевіряє відповідно.

б) Існує NP-відношення R і пара $(x,w) \in R$, причому x є спільним входом для P і V, а w — секретним для P.

в) Протокол складається із наступних кроків:

1) P обирає випадкове значення r і отримує $t = Commitment(x, w, r)$. Значення t відправляється до V.

2) V обирає випадкове значення $c = Challenge(\cdot)$ і відправляє P.

3) P відправляє V значення $s = Response(x, w, c, r)$.

4) V вирішує, повертати значення 1 або 0 базуючись на отриманих даних.

У цих кроках $Commitment$, $Challenge$, $Response$ — деякі поліноміальні у часі алгоритми.

Визначення 2.4. *Нехай $R(x, w)$ — NP-відношення для деякого протоколу P, що має σ-структуру. Протокол P називається Σ-протоколом тоді й тільки тоді, коли виконуються наступні властивості:*

а) Повнота: $\Pr[(\mathcal{P},\mathcal{V})(x) = 1|(x,w) \in R] \geq 1 - \epsilon$, де ϵ можна знехтувати.

б) Коректність: $\Pr[(\tilde{\mathcal{P}},\mathcal{V})(x) = 1|(x,w) \notin R] \leq \epsilon$, у випадку, коли P - нечесний. Ця властивість означає, що якщо пара (x, w) не належить R, то V видасть 1 з імовірністю не більшою за ϵ.

в) Стійка можливість діставання знань: для будь-якого x і будь-якої пари розмов (t, c, s) та (t, c', s'), для яких було повернуто 1, можна за поліноміальний час обчислити пару (x, w') таку, що $(x, w') \in R$.

г) Нерозголошення для чесного перевіряючого: існує поліноміальний у часі алгоритм M, який для входу x та випадкового c видає розмову (t, c, s), для якої було повернуто 1, причому ці розмови мають розподіл, що є поліноміально нерозрізрюваним із розподілом справжніх розмов між P і V для входу x.

У [12] можна побачити, як з Σ-протоколу є можливим побудувати

безпечний протокол доведення без розголошення за допомогою так званої OR-конструкції. Наведемо тут без доведення стійкості визначення цієї конструкції та процедуру побудови протоколу доведення без розголошення.

Визначення 2.5. *Нехай $\mathcal{P}$ — Σ-протокол для деякого NP-відношення $R(x, w)$. Тоді OR-конструкцією для такого протоколу називається протокол, що дозволяє P, маючи на вході деяку пару (x_0, x_1), довести V те, що він знає деяке w, таке, що виконується одна з наступних умов:*

$$(x_0, w) \in R,$$
$$(x_1, w) \in R,$$

без розкриття яка саме з них виконується.

У [12] наведено алгоритм побудови OR-конструкції з довільного Σ-протоколу.

Теорема 2.6. *Нехай $\mathcal{P}$ — Σ-протокол для деякого NP-відношення $R(x, w)$. Нехай x є спільним входом для P і V, а w — секретним для P. Тоді наступний протокол дозволяє P довести V без розголошення те, що він дійсно знає w:*

а) V запускає деякий генератор G на вході 1^k, де k — довжина x і отримує $(x', w') \in R$.

б) V відправляє x' до P і доводить йому (зауважимо, що на цьому кроці V і P тимчасово змінюють ролі) використовуючи $\mathcal{P}$ те, що він знає w'.

в) За умови успіху попереднього кроку, P використовує OR-конструкцію для доведення, що він знає w або w'.

Таким чином, для задачі побудови системи ID-based групового шифрування достатньо визначити відповідний Σ-протокол. Зробимо це.

Визначення 2.7. *Σ-протоколом для схеми ID-based групового шифрування з лазівкою називається протокол $\mathcal{P}$ між P, що провів шифрування і доводить правильність шифротексту і V, що перевіряє. Цей протокол має наступні кроки:*

а) P випадково обирає $\overline{s}, \overline{ID} \in_R \mathbb{Z}_p$. Після цього P обчислює і відправляє V наступні значення:

$$\overline{C_{10}} = g_1^{\overline{s}} g^{-\overline{s} \cdot ID},$$
$$\overline{C_{11}} = e(g,g)^{\overline{s}},$$
$$\overline{C_{20}} = g_1^{\dagger \overline{s}} g^{\dagger - \overline{s} \cdot ID},$$
$$\overline{C_{21}} = e(g^{\dagger},g^{\dagger})^{\overline{s}}.$$

б) V обирає $c \in_R \mathbb{Z}_p$ і відправляє його P.

в) P обчислює і відправляє V наступні значення:

$$r_1 = \overline{s} + cs \mod p,$$
$$r_2 = -\overline{s} \cdot ID - cs \cdot ID \mod p.$$

г) V перевіряє виконання наступних умов:

$$e(g,g)^{r_1} = C_{11}^c \overline{C_{11}}$$
$$e(g^\dagger, g^\dagger)^{r_1} = C_{21}^c \overline{C_{21}}$$
$$g_1^{r_1} g^{r_2} = C_{10}^c \overline{C_{10}}$$
$$g_1^{\dagger r_1} g^{\dagger r_2} = C_{20}^c \overline{C_{20}}$$

У разі, якщо всі ці умови виконані, V повертає "прийняття"(0), інакше "відмову"(1).

Доведення того, що цей протокол є Σ-протоколом, а саме, має властивості повноти, коректності, стійкої можливості діставання знань, нерозголошення для чесного перевіряючого, наведені у наступному розділі.

Це доведення дає змогу гарантувати неможливість формування некоректного шифротексту та уможливлює поєднання двох криптосистем у спільний протокол ID-based групового шифрування з лазівкою, як було зазначено у загальному описі.

Висновки до розділу 2

У даному розділі було наведено мотивацію задачі побудови схеми ID-based групового шифрування з лазівкою та розглянуто деякі типові приклади, де застосування такої схеми є доцільним.

Було запропоновано власну модифікацію схеми ID-based групового шифрування для забезпечення наявності лазівки, що контролюється менеджером групи, у шифротексті. Наведено загальний опис цієї схеми. Також наведено її детальний опис разом із деякими визначеннями, зокрема визначенням Σ-прооколів, що роблять можливим доведення її коректності. У наступному розділі таке доведення буде наведено.

3 ДОВЕДЕННЯ ВЛАСТИВОСТЕЙ СХЕМИ

3.1 Коректність схеми

Доведемо коректність розшифрування зашифрованого повідомлення. Для цього спочатку доведемо наступну властивість білінійних пар:

Теорема 3.1. *Розглянемо циклічну мультиплікативну групу* $\mathbb{G}$ *з генератором* g *та циклічну мультиплікативну групу* $\mathbb{G}_T$. *Нехай* $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ — *ефективне білінійне відображення,* $a, b, c \in \mathbb{G}$. *Тоді:*

$$e(ab, c) = e(a, c) \cdot e(b, c)$$

Доведення. Оскільки група $\mathbb{G}$ є циклічною з генератором g, то існують $x, y, z \in \mathbb{Z}$, такі, що:

$$a = g^x, b = g^y, c = g^z.$$

Тоді:

$$\begin{aligned} e(ab, c) &= e(g^x g^y, g^z) = e(g^{x+y}, g^z) = e(g, g)^{(x+y)z} = \\ &= e(g, g)^{xz+yz} = e(g,g)^{xz} \cdot e(g,g)^{yz} \\ &= e(g^x, g^z) \cdot e(g^y, g^z) = e(a, c) \cdot e(b, c). \end{aligned}$$

Тепер наведемо доведення коректності розшифрування повідомлення, а

саме, що (неформально):

$$DEC(\cdot, ENC(\cdot, M, \cdot), \cdot) = M.$$

Доведення. Згідно з визначенням алгоритму DEC, маємо:

$$C_{12} \cdot e\,(C_{10}{,}h_{ID})\, C_{11}^{r} = M \cdot e(g,h)^{-s} \cdot e(g_1^s g^{-s \cdot ID}, h_{ID}) =$$
$$= M \cdot e(g,h)^{-s} \cdot e(g_1^s g^{-s \cdot ID}, (hg^{-r})^{\frac{1}{\alpha - ID}}) \cdot e(g,g)^{sr} =$$
$$= M \cdot e(g,h)^{-s} \cdot e(g^{s(\alpha - ID)}, h^{\frac{1}{\alpha - ID}} g^{-\frac{r}{\alpha - ID}}) \cdot e(g,g)^{sr} =$$
$$= M \cdot e(g,h)^{-s} \cdot e(g,h)^{s} \cdot e(g,g)^{-sr} \cdot e(g,g)^{sr} = M.$$

3.2 Безпека компонентів схеми

Для визначення безпеки криптосистеми використовується модель зловмисника $\mathcal{A}$, що може робити адаптивні запити до набору деяких оракулів. Наведемо визначення даних оракулів:

– **Extract** — отримує на вхід ідентифікатор користувача ID, повертає відповідний секретний ключ SK_{ID}.

– **Corruption** — отримує на вхід відкритий ключ менеджера групи PK_{GM}, повертає відповідний закритий ключ менеджера групи SK_{GM}.

– **Encryption** — отримує на вхід набір (PK_{GM}, ID, M). Повертає відповідний шифротекст C.

– **Decryption** — отримує на вхід правильно сформований шифротекст

C, повертає відповідний відкритий текст M.

– **Trace** — отримує на вхід правильно сформований шифротекст C, повертає ідентифікатор отримувача цього шифротексту ID.

Для захисту повідомлення та ідентичності отримувача пропонуються наступні визначення:

Визначення 3.2. *Криптосистема називається* семантично безпечною, *якщо шифротекст не може надати поліноміально обмеженому зловмиснику інформацію про відкритий текст.*

Визначення 3.3. *Криптосистема називається семантично анонімною, якщо шифротекст не може надати поліноміально обмеженому зловмиснику інформацію про ідентичність отримувача.*

Наступне визначення призначене для надання можливості адміністратору групи визначити реального отримувача повідомлення

Визначення 3.4. *Криптосистема називається* такою, що має властивість відслідковуваності, *якщо жоден поліноміально обмежений зловмисник не може сформувати допустимий шифротекст із неправильним адресатом*

Наведемо уточнюючу формалізацію даних визначень.

Визначення 3.5. *Схема ID-based групового шифрування має властивості семантичної анонімності та семантичної безпеки щодо адаптивних атак з вибором особистості та адаптивних атак з вибором відкритого тексту, якщо жоден поліноміально обмежений зловмисник A не має суттєвої переваги у наступній грі:*

а) Будується система за допогою алгоритму ParaGen(λ). Цей алгоритм генерує системні параметри Params *та головний ключ* MSK. *Зловмисник отримує лише* Params.

б) Зловмисник робить адаптивні запити $ID_1, ID_2, ...$ *до оракулу* ***Extract****, отримуючи відповідні секретні ключі* $SK_{ID_1}, SK_{ID_2}, ...$

в) Зловмисник обирає два ідентифікатори ID_0, ID_1 *для яких він не робив запити на попередньому кроці та два відкритих тексти однакової довжини* M_0, M_1. *Незалежно від цього генеруються невідомі зловмиснику випадкові біти* $b, c \in \{0,1\}$. *Шифротекст* $C = Enc(Params, ID_b, M_c)$ *відправляється зловмиснику.*

г) Повторюється крок б), з умовами що запит не містить $ID_{1,2}$ *та не можна робити запити до оракулу Trace.*

д) Зловмисник повертає біти $b', c' \in \{0,1\}$. *Зловмисник виграє, якщо* $b = b'$ *та* $c = c'$.

Перевага зловмисника при цьому визначається як:

$$Adv_A(\lambda) = \left| \Pr\left[b = b' \wedge c = c'\right] - \frac{1}{4} \right|$$

Суттєвість переваги визначається з огляду на обчислювальну складність при виборі конкретної групи для реалізації криптосистеми.

У даній роботі для шифрування обох частин шифротексту використовується конструкція I публікації Джентрі та ін. [10]. Ця конструкція для доведення секретності покладається на доповнене вибіркове білінійне експоненційне q-припущення Діфі-Геллмана, визначене в розділі 2 цієї роботи.

За умови практичної реалізації у групі, у якій виконується доповнене вибіркове білінійне експоненційне q-припущення Діфі-Геллмана, визначене в розділі 2 цієї роботи, ця криптосистема має властивість ANO-IND-ID-CPA безпеки, що є доведеним у [10]. У термінах, визначених вище, це означає, що ця схема має властивості *семантичної анонімності* та *семантичної безпеки* за умови проведення атак з адаптивним вибором особистості та адаптивним вибором відкритого тексту.

Отже, виходячи з визначення 3.5 та опису запропонованої схеми, для того, щоб можна було стверджувати, що запропонована схема ID-based групового шифрування з лазівкою має властивості семантичної анонімності та семантичної безпеки щодо адаптивних атак з вибором особистості та адаптивних атак з вибором відкритого тексту, необхідно довести, що протокол доведення без розголошення є:

– таким, що не розкриває зашифрований ідентифікатор

– таким, що дійсно доводить однаковість ідентифікаторів для обох частин шифротексту

Це досягається за рахунок побудови протоколу доведення без розголошення на основі Σ-протоколу. Отже, достатньо довести, що наведений протокол є дійсно Σ-протоколом. Зробимо це.

3.3 Протокол доведення без розголошення

Доведемо те, що протокол з визначення 2.7 справді є Σ-протоколом у сенсі визначення 2.4. Для цього по черзі розглянемо властивості, якими він

має володіти для цього.

– *Стійка можливість діставання знань.* Доведемо, що існує алгоритм обчислення пари $(x, w') \in R$ для будь-якого x і будь-якої пари пов'язаних з x розмов (t, c, s) та (t, c', s'), для яких було повернуто 1.

Доведення. Алгоритм буде виконувати роль V у протоколі, але повторить діалог з P двічі. При цьому він використовує різні значення $c, c' \neq c \in_R \mathbb{Z}_P$. Відповідно, після діалогів необхідно обчислити секрети s, ID. Маємо такі рівняння для секрету s:

$$r_1 = \overline{s} + cs \mod p$$
$$r_1' = \overline{s} + c's \mod p.$$

Звідси знаходимо s, як:

$$s = \frac{r_1 - r_1'}{c - c'} \mod p.$$

Аналогічно для $-s \cdot ID$:

$$r_2 = -\overline{s} \cdot \overline{ID} - cs \cdot ID \mod p$$
$$r_2' = -\overline{s} \cdot \overline{ID} - c's \cdot ID \mod p$$
$$-s \cdot ID = \frac{r_2 - r_2'}{c - c'} \mod p.$$

Для знаходження ID, знаючи s, знаходимо власне ID.

– *Нерозголошення для чесного перевіряючого*. Симулятору достатньо обрати $s, \overline{C_{10}}, \ldots, \overline{C_{21}}$ випадково, незалежно і рівноімовірно із множини допустимих значень. Отриману розмову неможливо буде відрізнити від реальної.

– *Повнота*. Доведення повноти напряму випливає з визначення протоколу.

– *Коректність*. Доведемо, що $\Pr[(\tilde{\mathcal{P}},\mathcal{V})(x) = 1|(x,w) \notin R] \leq \epsilon$, у випадку, коли P - нечесний.

Для нашого випадку ця вимога означає, що ймовірністю успішного проходження протоколу тоді, коли C_1 і C_2 зашифровані для різних ідентифікаторів $ID_1 \neq ID_2$ можна знехтувати.

Доведення. Нехай P - нечесний, і формує шифротексти $C_{10} = g_1^s g^{-s \cdot ID}$, $C_{20} = g_1^{\dagger\overline{s}} g^{\dagger - \overline{s} \cdot ID'}$, причому $ID \neq ID'$. Тоді під час виконання протоколу P обирає $-\overline{s} \cdot \overline{ID}_1, -\overline{s} \cdot \overline{ID}_2$.

Лема. $\overline{ID}_1 \neq \overline{ID}_2$. *Доведення.* Якщо $\overline{ID}_1 = \overline{ID}_2$, то

$$
\begin{aligned}
& g_1^{r_1} g^{r_2} = C_{10} C_{10}^c, \\
& g_1^{\dagger r_1} g^{\dagger r_2} = C_{20} C_{20}^c, \\
& r_2 \equiv -\overline{s} I\overline{D}_1 + (-s \cdot ID)c \bmod p, \\
& r_2 \equiv -\overline{s} I\overline{D}_2 + (-s \cdot ID')\, c \bmod p
\end{aligned}
$$

А значить, що $ID = ID'$.

Доведено.

Згідно з визначенням протоколу, P обчислює:

$$\overline{C_{10}} = g_1^{\overline{s}} g^{-\overline{s} \cdot \overline{ID_1}}$$
$$\overline{C_{20}} = g_1^{\dagger \overline{s}} g^{\dagger - \overline{s} \cdot \overline{ID_2}},$$

Для успішного виконання протоколу необхідно, щоб одночасно виконувались наступні умови:

$$\begin{cases} g_1^{r_1} g^{r_2} = C_{10}^c \overline{C_{10}} \\ g_1^{\dagger r_1} g^{\dagger r_2} = C_{20}^c \overline{C_{20}} \end{cases}$$

Це може відбутись тільки в тому випадку, коли:

$$-\overline{s}\overline{ID}_1 + (-s \cdot ID)c \equiv -\overline{s}\overline{ID}_2 + (-s \cdot ID')\, c \bmod p$$

Для цього потрібно, щоб c дорівнювало $\frac{\overline{s}\left(\overline{ID}_1 - \overline{ID}_2\right)}{s(ID' - ID)}$.

Проте, оскільки c обирається V випадково і рівноймовірно, ймовірність цього дорівнює $\frac{1}{p}$ і є несуттєвою.

Доведено.

Висновки до розділу 3

У даному розділі було проведено доведення властивостей запропонованого протоколу ID-based групового шифрування з лазівкою, зокрема таких його частин, як протоколу доведення без розголошення, а саме, Σ-протоколу, що лежить в його основі. Було визначено модель, у якій складові частини протоколу є стійкими, та наведено обґрунтування його загальної стійкості у цій моделі.

ВИСНОВКИ

В даній роботі досліджено протоколи відправлення зашифрованих повідомлень із забезпеченням властивості анонімності ключа. Проведено аналіз ID-based протоколів групового шифрування та протоколів групового шифрування з лазівкою.

Визначивши ключові аспекти можливого застосування, наведено мотивацію доцільності побудови протоколу ID-based групового шифрування з лазівкою. Запропоновано відповідний протокол. Проведено роботу з надання оглядового опису відповідного протоколу. Наведено формальне визначення складових частин протоколу та описано їх роботу в формальних деталях.

На основі наведеного визначення протоколу проведено аналіз його властивостей, зокрема коректності та безпеки. Було визначено модель безпеки та відповідність складових частин протоколу та протоколу в цілому цій моделі.

Доцільними напрямками подальшої роботи можуть бути:

– Практична реалізація запропонованого протоколу та оцінка його часової та просторової складності.

– Поглиблений аналіз властивостей безпеки наведеного протоколу ID-based групового шифрування з лазівкою.

– Побудова покращеного протоколу із використанням інших складових частин, зокрема, підпротоколу ID-based шифрування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Boneh, Dan. The Decision Diffie-Hellman problem [Text] / Dan Boneh // Algorithmic Number Theory / Ed. by Joe P. Buhler. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1998. — P. 48–63.

2. Diffie, Whitfield. New directions in cryptography [Text] / Whitfield Diffie, Martin Hellman // IEEE transactions on Information Theory. — 1976. — Vol. 22, no. 6. — P. 644–654.

3. Merkle, Ralph C. Secure Communications over Insecure Channels [Text] / Ralph C. Merkle // Commun. ACM. — 1978. — Apr. — Vol. 21, no. 4. — P. 294–299. — Access mode: http://doi.acm.org/10.1145/359460.359473.

4. Rivest, R. L. A Method for Obtaining Digital Signatures and Public-key Cryptosystems [Text] / R. L. Rivest, A. Shamir, L. Adleman // Commun. ACM. — 1978. — Feb. — Vol. 21, no. 2. — P. 120–126. — Access mode: http://doi.acm.org/10.1145/359340.359342.

5. Kiayias, Aggelos. Group Encryption [Text] / Aggelos Kiayias, Yiannis Tsiounis, Moti Yung // Advances in Cryptology – ASIACRYPT 2007. — 2007. — Vol. 4833. — P. 181–199. — Access mode: http://dx.doi.org/10.1007/978-3-540-76900-2{_}11.

6. Group Decryption [Text] / Bo Qin, Qianhong Wu, Willy Susilo [et al.]. — 2007. — P. 1–18.

7. Traceable Group Encryption [Text] / Benoît Libert, Moti Yung, Marc Joye, Thomas Peters / Ed. by Hugo Krawczyk. — Berlin, Heidelberg : Springer Berlin Heidelberg, 2014. — Vol. 8383 of Lecture Notes in Computer Science. — P. 592–610. — Access mode: http://link.springer.com/10.1007/

978-3-642-54631-0{_}34.

8. Identity-based group encryption [Text] / Xiling Luo, Yili Ren, Jingwen Liu [et al.] // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). — Vol. 9723. — [S. l.] : Springer, Cham, 2016. — jul. — P. 87–102. — Access mode: http://link.springer.com/10.1007/978-3-319-40367-0{_}6.

9. Boneh, Dan. Identity-Based Encryption from the Weil Pairing [Text] / Dan Boneh, Matthew Franklin // SIAM Journal on Computing. — 2003. — Vol. 32, no. 3. — P. 586–615. — 9780201398298.

10. Gentry, Craig. Practical Identity Based Encryption Without Random Oracles [Text] / Craig Gentry. — 2006. — P. 445–464.

11. Meffert, Dennis. Bilinear Pairings in Cryptography [Text] / Dennis Meffert // Science. — 2009.

12. Damgard, Ivan. On Σ-protocols [Text] / Ivan Damgard // Lecture notes for CPT. — 2002. — Access mode: http://www.cs.au.dk/{~}ivan/Sigma.pdf.